Mathematics, Computing and Technology
M303 Further Pure Mathematics

Specimen Solutions

Formative solutions for TMA01 202xJ

TMA 01

Solution to Question 8 – 14 marks

(a) (i) 0 or $0 + 0\sqrt{-7}$

(ii) Examples include: $2 + 2\sqrt{-7}$, $4 + 4\sqrt{-7}$ or $4 + 2\sqrt{-7}$.

(iii) Examples include 1, $\sqrt{-7}$, $1 + \sqrt{-7}$, $2 + \sqrt{-7}$ and $1 + 2\sqrt{-7}$.

(iv) Determined by (ii) and (iii).
For example $(2 + 2\sqrt{-7}) +_G 1 = 3 + 2\sqrt{-7}$,
$(2 + 2\sqrt{-7}) +_G \sqrt{-7} = 2 + 3\sqrt{-7}$ and
$(2 + 2\sqrt{-7}) +_G (2 + \sqrt{-7}) = 4 + 3\sqrt{-7}$

(b) We need to check that each of the group axioms
Definition 1.1 of Chapter 5, page 5 of book B hold.

Closure

We need to show that adding two arbitrary elements of G (using $+_G$) gives us an element of G.

Let $a + b\sqrt{-7}$ and $x + y\sqrt{-7}$ be arbitrary elements of G, with a, b, x and $y \in \mathbb{Z}$. Then $(a + b\sqrt{-7}) +_G (x + y\sqrt{-7}) = (a + x) + (b + y)\sqrt{-7}$ which is in G since $a + b$ and $x + y$ are in $\mathbb{Z}$.

Therefore $(G, +_G)$ is closed.

Identity

By part (a)(i) G has an identity.

Inverses

We need to show that an arbitrary element of G has an inverse. This means that we need to take an arbitrary element, $a + b\sqrt{-7}$ of G and find an element $x + y\sqrt{-7}$ such that $(a + b\sqrt{-7}) +_G (x + y\sqrt{-7}) = 0$ (since 0 is the identity of G).

Since $-a$ and $-b$ are in $\mathbb{Z}$, we know that $(-a) + (-b)\sqrt{-7} \in G$ and $(a + b\sqrt{-7}) +_G ((-a) + (-b)\sqrt{-7}) = 0$.

Therefore each element of G does have an inverse in G.

Associativity

Addition in $\mathbb{Z}$ is associative so $+_G$ is associative.

Therefore all four axioms hold and $(G, +_G)$ is a group.

For similar examples see
Worked Exercise 1.3 and Exercise 1.1 of Book B, page 7 and practice quiz 2.

(c) As suggested by the question we use the subgroup criteria (with additive notation) ***Proposition 2.5 of Book B, page 19***

For (a) we note that $H \neq \emptyset$ since it contains the identity.

For (b) we need to take two arbitrary elements of H, say $2a + 2b\sqrt{-7}$ and $2x + 2y\sqrt{-7}$, and show that $2a + 2b\sqrt{-7} +_G (-2x) + (-2y)\sqrt{-7}$ is also in H.

If $2a + 2b\sqrt{-7}$ and $2x + 2y\sqrt{-7}$ are arbitrary elements of H, then $(2a + 2b\sqrt{-7}) +_G (-2x + -2y\sqrt{-7}) = 2(a - x) + 2(b - y)\sqrt{-7}$.

Copyright © 2020 The Open University

However $a-x$ and $b-y$ are both in $\mathbb{Z}$ and so (by definition), $2(a-x)+2(b-y)\sqrt{-7} \in H$.

and so H is a subgroup by the subgroup criterion

HB page 25/26, Proposition 2.2 or 2.4 or 2.5 of Chapter 5

(d) G is abelian so all subgroups are normal ***Exercise 3.2 of Chapter 5***

(e) The elements of G/H are cosets of the form $(a+b\sqrt{-7})+H$.

Two cosets, $(a+b\sqrt{-7})+H$ and $(a'+b'\sqrt{-7})+H$ will be equal if $(a+b\sqrt{-7})-(a'+b'\sqrt{-7}) \in H$. This happens if, and only if, $(a-a') \in 2\mathbb{Z}$ and $(b-b') \in 2\mathbb{Z}$.

Therefore the cosets will be all elements of the form $a+b\sqrt{-7}$ where $a \in \{0,1\}$ and $b \in \{0,1\}$ giving the $2 \times 2 = 4$ choices.

These are:

$$\{0+H, 1+H, \sqrt{-7}+H, 1+\sqrt{-7}+H\}$$

The Cayley table is

	H	$1+H$	$\sqrt{-7}+H$	$1+\sqrt{-7}+H$
H	H	$1+H$	$\sqrt{-7}+H$	$1+\sqrt{-7}+H$
$1+H$	$1+H$	H	$1+\sqrt{-7}+H$	$\sqrt{-7}+H$
$\sqrt{-7}+H$	$\sqrt{-7}+H$	$1+\sqrt{-7}+H$	H	$1+H$
$1+\sqrt{-7}+H$	$1+\sqrt{-7}+H$	$\sqrt{-7}+H$	$1+H$	H

(f) No (There is no element of order 4. In fact $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$)

Solution to Question 9 – 10 marks

Remarks:

When given a problem like this, a natural thing to do is to try and solve it in particular cases.

For example, if there is only one blue-eared alien, then, following the outsider's announcement, it will look around, see that no other aliens have blue ears and immediately conclude that it must have blue ears. Hence the following revolution at 6am, it departs the planetoid.

If there are two blue-eared aliens, then following the outsider's announcement, they will both look around and each see one alien with blue ears. However each of them will not be able to conclude that they also have blue ears. However at 6am the following revolution, no aliens depart and had there been only one alien with blue ears, then it would have left. Hence at this point, the (two) aliens with blue ears deduce that they each have blue ears and at 6am on the following revolution, they depart the planetoid.

This argument extends to any number of aliens...

(a) At 6am on the kth revolution following the outsider's announcement, the k aliens with blue ears will all leave the planetoid.

(b) Let $E\colon \mathbb{N} \to \mathbb{N}$ be the function that, given k, determines how many revolutions until the k aliens with blue ears depart. (It could be that such a function does not exist in which case we would hope to derive a contradiction but, as we shall shortly see, this is not the case.)

We use the Principle of Mathematical Induction p18 of Chapter 1, HB p14 to show that $E(k) = k$.

Suppose that $k = 1$. Then, following the outsider's announcement, the (sole) alien with blue ears will look around and observe that none of the other aliens have blue ears. Since the outsider said that there are aliens with blue ears, the

alien deduces that they must have blue ears and so departs the planetoid at 6am the following revolution. Hence $E(1) = 1$.

Now fix $k \in \mathbb{N}$ and suppose that we have shown that $E(k) = k$ — that is, if there are k aliens with blue ears, then they depart the planetoid at 6am on the kth revolution following the outsider's announcement.

We show that this implies $E(k+1) = k+1$.

So suppose that there are $k+1$ aliens with blue ears. Then each of them can see (exactly) k aliens with blue ears and so when, on day k, nobody departs (in line with the induction hypothesis), each of them correctly deduces that they themselves also have blue ears and so on the following revolution, departs the planetoid. This is true for all $k+1$ aliens, and so we conclude that $E(k+1) = k+1$.

Hence we conclude that $E(k) = k$ for each $k \in \mathbb{N}$.

Solution to Question 10 – 13 marks

(a) If α is a root of a polynomial with integer coefficients that has degree 1, then there is a polynomial $P(x)$ of the form $P(x) = a_1x + a_0$ with $a_1, a_0 \in \mathbb{Z}$, $a_1 \neq 0$ and $P(\alpha) = 0$. That is, with $a_1\alpha + a_0 = 0$ and this rearranges to give $\alpha = -a_0/a_1 \in \mathbb{Q}$. However we are told that none of $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{2}+\sqrt{3}$ is rational, and so we conclude that they can not be roots of polynomials with integer coefficients of degree 1.

(b) If p is prime, then $P_p(x) = x^2 - p$ is a polynomial with integer coefficients of degree 2 for which $\sqrt{p}$ is a root.

(c) If $P_p(x) = Q(x) \cdot R(x)$, where Q and R are polynomials of degree one, then

$$Q(x) = ax + b \text{ and } R(x) = cx + d,$$

where $a, b, c, d \in \mathbb{Z}$ with both $a, c \neq 0$. By multiplying out we see that

$$x^2 - p = (ac)x^2 + (ad + bc)x + bd$$

and on equating coefficients we see that $ac = 1$, $bd = -p$ and $ad = -bc$. Hence either $a = c = 1$ or $a = c = -1$, giving $b = -d$ in either case. Thus $-b^2 = -p$, which means that $b^2 = p$. But no integer squared can equal a prime, and so no such b exists, meaning P_p cannot be written as a product of lower degree polynomials.

In fact, for any $n \in \mathbb{N}$, $P_n(x) = x^2 - n$ is a polynomial for which $\sqrt{n}$ is a root. Notice that if $n = m^2$, then we can factorise P_n as a product of two polynomials of degree 1 that have integer coefficients: $P_n(x) = (x - m)(x + m)$.

(d) There is a general technique for finding such polynomials: if $\alpha = \sqrt{2}+\sqrt{3}$, then

$$(\alpha - \sqrt{2})^2 = (\sqrt{3})^2 = 3$$

and so

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = 3,$$

which rearranges to give

$$\alpha^2 - 1 = 2\sqrt{2}\alpha$$

and squaring both sides of this expression gives

$$(\alpha^2 - 1)^2 = 8\alpha^2,$$

which expands and rearranges to give $\alpha^4 - 10\alpha^2 + 1 = 0$. Hence a polynomial with integer coefficients that has α as a root is $P(x)$ given by

$$P(x) = x^4 - 10x^2 + 1.$$

This polynomial has degree 4.

Solution to Question 11 – 13 marks

(a) To solve this question, we need to assume that $\text{hcf}(p, q) = 1$. (So the condition in the question that p and q are assumed to be distinct, odd primes is more than we need.)

If $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$ then, since $\text{hcf}(p, q) = 1$, $x^2 \equiv 1 \pmod{pq}$ by Theorem 1.6 of Chapter 3.

On the other hand, if $x^2 \equiv 1 \pmod{pq}$ then, since p divides pq, $x^2 \equiv 1 \pmod{p}$ and similarly $x^2 \equiv 1 \pmod{q}$.

(b) Lagrange's Theorem (Theorem 4.3 of Chapter 4) guarantees that this congruence, of degree 2 and with prime modulus, has at most two solutions modulo p. However $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$ are certainly solutions and are distinct as p is odd, and consequently these must be the only two.

(c) Any solution of $x^2 \equiv 1 \pmod{pq}$ must be a solution of one of the four simultaneous pairs:

$$x \equiv 1 \pmod{p} \text{ and } x \equiv 1 \pmod{q}$$
$$x \equiv 1 \pmod{p} \text{ and } x \equiv -1 \pmod{q}$$
$$x \equiv -1 \pmod{p} \text{ and } x \equiv 1 \pmod{q}$$
$$x \equiv -1 \pmod{p} \text{ and } x \equiv -1 \pmod{q}$$

The Chinese Remainder Theorem ensures that each of these systems has a unique solution modulo pq. Moreover these solutions are different since a number cannot be congruent to both 1 and -1 modulo an odd prime. Therefore

$$x^2 \equiv 1 \pmod{pq} \text{has four solutions.}$$

(d) $95 = 5 \cdot 19$, so we solve the four simultaneous systems

$$x \equiv 1, -1 \pmod{5} \text{ and } x \equiv 1, -1 \pmod{19}$$

Now,

$$x \equiv 1 \pmod{5} \text{ and } x \equiv 1 \pmod{19} \Rightarrow x \equiv 1 \pmod{95}$$
$$x \equiv 1 \pmod{5} \text{ and } x \equiv -1 \pmod{19} \Rightarrow x \equiv 56 \pmod{95}$$
$$x \equiv -1 \pmod{5} \text{ and } x \equiv 1 \pmod{19} \Rightarrow x \equiv 39 \pmod{95}$$
$$x \equiv -1 \pmod{5} \text{ and } x \equiv -1 \pmod{19} \Rightarrow x \equiv 94 \pmod{95}$$

So the four solutions are $x \equiv 1, 56, 39, 94 \pmod{95}$.

(e) Lagrange's Theorem (Theorem 4.3 of Chapter 4) is only applicable in the case of congruences to a prime modulus. As this example shows, working to a composite modulus the number of solutions of a congruence can exceed the degree.

Chapter 3, Page 145, Worked Exercise 3.3

Chapter 3, Page 156, Worked Exercise 4.4